CYBER INCIDENT RESPONSE PLAYBOOK BASED ON MITRE ATT&CK

Contents

Impact - Data Encrypted For Impact - Ransomware

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Confirm backups are free of malware
4. Establish ability to pay ransoms w/cryptocurrency
5. Obtain decryption keys for ransomware variants
6. Confirm cybersecurity insurance coverages
7. Conduct ransomware simulations
8. Conduct phishing simulations
9. Conduct user awareness training
10. Conduct response training (this PBC)
11. Examine file shares for loose/open privileges
12. Maintain Antivirus/EDR application updates
13. Create network segmentation
14. Log traffic between network segments
15. Incorporate threat intelligence
16. Incorporate deception technology
17. Perform routine inspections of asset backups
18. Validate proper functionality

(I) Identification

1. Monitor for:
    a. Ransomware notes/messages
    b. Unusual file extensions or maliciousextensions
    c. User reports of files being corrupt or notreadable d. Emails with suspicious attachments
    d. Unusual DNS traffic
    e. High velocity renaming of files
    f. CPU spikes on file sharing systems
    g. Unusual userland executable binaries
    h. Anomalous network connections on hosts
    i. Firewall denies to well known file sharingports
    j. Network connections to known C2 andexploit kit locations l. Use of TOR or I2P
2. Investigate and clear ALL alerts of possible ransomware
    a. IDS/IPS
    b. Antivirus/EDR
    c. Threat intelligence
    d. Deception technology

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Locate and isolate the assets responsible for encrypting files
5. Isolate impacted file sharing systems
6. Close the attack vector
7. Fortify non-impacted file sharing systems
8. Fortify non-impacted critical assets
9. Issue perimeter enforcement for known threat actor locations
10. Deploy EDR hunter/killer agents and terminate offending processes

(E) Eradication

1. Close the attack vector

2. Patch asset vulnerabilities
3. Re-image impacted assets
4. Inspect all assets for IOC consistent with the attack profile
5. Inspect user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery
7. Implement newly obtained threat signatures

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore from known clean backups
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Avoid opening email and attachments from unfamiliar senders
4. Avoid opening email attachments from senders that do not normally include attachments

Initial Access - Exploit Enterprise Resources - Mobile Device SIM Attacks

(P) Preparation

1. Favor use of authenticator apps over SMS
2. Create a strong account PIN or Passphrase
3. Use a dedicated number for high-value accounts a. Alternative: Use a free Google Voice number
4. Use a password manager
5. Never store passwords, payment methods, etc. in your phone's browser
6. Prepare backup communications ability to allow you to respond more quickly to a compromise
7. Hangouts, GVoice, Skype, Line, etc.
8. Conduct user awareness training
9. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
   a. Unexplained, prolonged loss of cell service
   b. Unexpected customer service calls, "Sorry we got disconnected …"
   c. Alerts about password/authentication changes to your accounts d. Alerts on your phone, "Are you trying to log in from , ?"

(C) Containment

1. Notify your mobile carrier as soon as you can
2. Explain the situation:
   a. "I am a high-value-target individual and my phone number was ported approximately 3 hours ago to a new SIM that I do not control …"
3. Request that the number be completely disabled:
   a. "Since this is an active situation, please remove my phone number from that SIM immediately, meaning no one can receive phone calls or text messages to my number"
4. Request that your number to be moved back to your SIM
   a. This may be more difficult than getting the number disabled
5. Record the employee's name/number and dates
6. Record all case/support ticket numbers
7. Request that all logs for your IMEI be saved
8. Change all of your passwords from a non-compromised trusted device
   a. Change your major email accounts first
   b. Prioritize: Most to least valuable
   c. Document your actions as you are conducting them, including times and screen shots

(E) Eradication

1. Request that your mobile service block all swap attempts for one week
2. See additional steps in "Containment"

(R) Recovery

1. Retain legal counsel
2. Contact appropriate law enforcement agencies
3. Contact affected business partners
   a. Follow the advice of your legal counsel
4. Retain the services of security professionals
5. Regain control of your various compromised accounts
   a. Every provider will be different
   b. Document dates, times, names, and steps

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Be aware of all 2FA options when setting up new accounts, disabling all weak, SMS- based options
3. Be aware that the vulnerability is with your mobile provider and you have limited control over it
    a. Focus instead on what you can control
    b. Defense-in-depth and compartmentalization of your accounts

Credential Access - Spearphishing - Phishing

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Perform routine phishing education
4. Conduct phishing simulations
5. Log network traffic
6. Log incoming and outgoing emails
7. Establish a method for users to report suspicious emails
8. Incorporate threat intelligence

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Emails with suspicious attachments
    c. Multiple identical emails sent from unknown sources d. Emails sent from typo domains
    d. Emails that fail SPF and/or DKIM
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Lock or reset the password of affected users if credentials were disclosed

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Inspect any attachments included in the emails
4. Perform Endpoint/AV scans on the systems of affected users
5. Review logs to identify other affected users

(R) Recovery

1. Verify any compromised credentials have been changed
2. Restore/re-image any systems with malware present
3. Blacklist sources of phishing emails
    a. Individual sending email addresses
    b. Entire sending domain, if appropriate
4. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Exfiltration - Automated Exfiltration - Data Theft

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Provide security awareness training to employees

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Unusual file system activity
    c. Unusual network activity
    d. Antivirus/endpoint alerts
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Temporarily remove affected systems from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users

(R) Recovery

1. Identify the malware strain used
2. Determine what data may have been uploaded
3. Verify any compromised credentials have been changed
4. Restore/re-image any systems with malware present
5. Scan other systems and logs for known Indicators of Compromise
6. Block IP addresses associated with the malware on perimeter firewalls

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Lateral Movement - Pass the Hash

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that servers and workstations are logging to a central location
5. Network segmentation and firewalls can help reduce impact
6. Disable NTLM authentication where possible
    a. SMB
    b. HTTP
    c. SMTP

(I) Identification

1. Monitor for:
    a. Unusual user activity
    b. Unexpected logins using NTLM
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Lock accounts suspected of having a compromised hash
6. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users
4. Review logs to identify other potential cases of passing the hash

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Change the passwords of any potentially compromised accounts
4. Determine the chain of events that led to the pass the hash incident
5. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Persistence - Create Account - Backdoor User Accounts

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that servers and workstations are logging to a central location
5. Verify that security software generates alerts when privileged accounts are created
6. Remove inactive/unused accounts

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Privileged account creation
    c. Unexpected permissions changes for accounts
2. Investigate and clear ALL alerts associated with the impacted assets
3. Review log activity of the newly created account and the account that was used to create it
4. Contact users out of band to inquire about new account

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Lock suspicious accounts
6. Lock any compromised accounts
7. Review the activity of newly created and compromised accounts
8. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Identify and close the initial attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users
4. Verify that any additional persistence mechanisms have been removed

(R) Recovery

1. Restore to the RPO within the RTO for affected systems
2. Address collateral damage
3. If the attacker gained Domain Admin access, reset the krbtgt user account's password

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professional

Initial Access - Trusted Relationship - Vendor Access to Infrastructure

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain a list of vendors with system or network access
4. Verify that vendors only have access to necessary systems and networks
5. Isolate vendor accessible systems from the rest of the network as much as possible
6. Routinely audit vendor network access and system accounts
7. Force vendor accounts to use multifactor authentication where possible
8. Ensure all systems and network devices log to a central location

(I) Identification

1. Monitor for:
    a. Vendor access during unusual hours/days
    b. Vendor access from unusual sources (i.e. geographic locations, IPs, etc.)
    c. Attempts by vendor accounts to access other systems/networks
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely review vendor activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Block access from the compromised vendor
6. Lock accounts associated with the compromised vendor
7. Inform vendor of detected activity
8. Inspect all potentially compromised systems for IOCs

(E) Eradication

1. Patch asset vulnerabilities
2. Perform Endpoint/AV scans on the systems of affected users
3. Review logs to determine extent of unauthorized activity

(R) Recovery

1. Restore to the RPO within the RTO for affected systems
2. Address collateral damage
3. Reset passwords for vendors accounts
4. Restore necessary vendor access when safe

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Persistence - Browser Extensions - Malicious Browser Extensions

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that workstations are logging to a central location
5. Log network traffic
6. Use Group Policy to whitelist approved browser extensions

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Antivirus/Endpoint alerts c. IDS/IPS alerts
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Identify the malicious extension
5. Issue perimeter enforcement for known threat actor locations
6. Remove the affected system from the network if necessary

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Check the system for other malicious/unapproved extensions
4. Remove the malicious extension from the system
5. Perform an antivirus scan on the affected system

(R) Recovery

1. Restore to the RPO within the RTO for affected systems
2. Address collateral damage
3. Determine how and why the extension was installed
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Money Mule Scams - CEO Fraud

(P) Preparation

1. Perform routine inspections of controls/weapons
2. Perform routine phishing education
3. Conduct phishing simulations
4. Establish procedures for verifying requested financial transactions out of band
5. Log incoming and outgoing emails
6. Establish a method for users to report suspicious emails

(I) Identification

1. Monitor for:
    a. Emails with suspicious attachments
    b. Multiple identical emails sent from unknown sources
    c. Emails sent from typo domains
    d. Emails that fail SPF and/or DKIM
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Review email logs to identify other affected users
6. Review relevant financial transactions

(E) Eradication

1. Contact financial institutions to halt/reverse transactions

(R) Recovery

1. Blacklist sources of phishing emails
    a. Individual sending email addresses
    b. Entire sending domain, if appropriate
2. Report the incident to the appropriate law enforcement agency

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professional

Persistence - Web Shells

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Disable script execution in directories where it is not required
5. Verify that web applications do not run with excessive privileges on the server
6. Use AppArmor, SELinux, or other mitigations where appropriate

(I) Identification

1. Monitor for:
    a. Unusual error messages in logs
    b. Unusual web traffic patterns
    c. Unexpected changes in websites' document roots
    d. IPS/IDS alerts
    e. Antivirus alerts
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Review web logs to identify instances of the web shell being accessed
5. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Scan web servers for other instances of web shells
4. Determine how the web shell was placed on the system
5. Reset any potentially compromised passwords
6. Review logs of any system the attacker may have accessed
7. Scan affected systems with antivirus/endpoint software

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Device Theft - Device Loss

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain an up to date inventory of electronic devices
4. Place asset tags on company owned devices
5. Make use of full disk encryption
6. Set password/pin policies on devices
7. Maintain the ability to remotely wipe devices
8. Be aware of any laws or contractual obligations requiring notification of data loss

(I) Identification

1. Monitor for:
    a. Employee reports of device theft/loss

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Determine:
    a. What data was stored on the device
    b. How data stored on the device is protected
    c. What remote data and services are accessible from the device
5. Change the passwords of any accounts used on the device
6. Review logs for unauthorized activity from the stolen/lost device or accounts associated with it
7. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Perform a remote wipe of the device

(R) Recovery

1. Restore to the RPO within the RTO
2. Notify third parties of data loss if appropriate
3. Notify law enforcement if appropriate
4. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Initial Access - Drive By Compromise

(P) Preparation

1. Patch browsers and other software regularly
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that workstations are logging to a central location
5. Log network traffic
6. Set up a proxy for web traffic
7. Use Group Policy to manage security related browser settings
8. Make use of Windows Defender Exploit Guard or other exploit mitigation tools

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Antivirus/Endpoint alerts
    c. IDS/IPS alerts
    d. User reports of unexpected behavior
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Systems believed to have been compromised should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform an antivirus scan on the affected system
4. Review logs and network traffic to identify any related malicious activity

(R) Recovery

Restore to the RPO within the RTO
Address collateral damage
Reset the passwords of any accounts in use on the compromised system

1. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Initial Access - External Remote Services – Unauthorized VPN and VDI Access

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Prohibit non-employees from accessing company devices
5. Ensure that all remotely accessible services are logging to a central location
6. Provide security awareness training to employees
7. Use multifactor authentication where possible
8. Ensure proper network segmentation/firewall rules are in place for remote users
9. Routinely audit remote system access

(I) Identification

1. Monitor for:
   (L) Lessons/OpportunitiesRemote access during unusual hours/days
   e. Remote access from unusual sources (i.e. geographic locations, IPs, etc.)
   f. Excessive failed login attempts
   g. IPS/IDS alerts
   h. Antivirus/Endpoint alerts
2. Investigate and clear ALL alerts associated with the impacted assets
3. Contact the user out of band to determine the legitimacy of the detected activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Block access from the compromised user
6. Lock accounts associated with the compromised user
7. Inspect all potentially compromised systems for IOCs

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform an antivirus scan on the affected system
4. Review logs and network traffic to identify any related malicious activity

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Impact - Defacement

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Verify that servers are backed up on a regular basis

(I) Identification

1. Monitor for:
   a. Unplanned changes to any websites
   b. Unusual error messages in logs
   c. Unusual web traffic patterns
   d. IDS/IPS alerts
   e. Antivirus alerts
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Temporarily take down the defaced website
5. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Review logs to determine the cause of the breach
2. Perform antivirus scans on affected systems
3. Review web servers and other systems for evidence of backdoors or lateral movement
4. Verify the integrity of any data the attackers had access to
5. Reset any potentially compromised passwords
6. Patch asset vulnerabilities

(R) Recovery

1. Restore the defaced content
2. Address collateral damage
3. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Impact - Inhibit System Recovery - Disabling Volume Shadow Service

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Ensure Antivirus/Endpoint Protection software is installed on workstations
5. Verify that important data is backed up regularly
6. Ensure that accounts with administrative privileges are only used when necessary

(I) Identification

1. Monitor for:
   a. Antivirus/endpoint alerts
   b. Log messages related to system recovery services being altered or disabled
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Temporarily remove the affected system from the network

(E) Eradication

1. Perform Endpoint/AV scans on affected systems
2. Review logs to determine the cause of the detected activity
3. Determine if any other systems or user accounts have been compromised
4. Check for altered or deleted files on the system and network shares
5. Reset any potentially compromised passwords
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Defense Evasion - Disabling Security Software

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on systems
4. Ensure that servers are logging to a central location
5. Verify that regular users don't have excessive permissions

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. An unusual absence of logs from security software
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Temporarily remove the affected system from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on affected users
4. Review logs to determine if any other systems are affected

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Defense Evasion - Install Root Certificate

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations and laptops
4. Ensure that servers and workstations are logging to a central location
5. Maintain a list of known good root certificates
6. Check pre-installed root certificates on new devices

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. An unusual absence of logs from security software
2. Periodically enumerate root certificates on devices and check for changes
3. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Remove the affected system from the network
5. Check for the presence of the root certificate on other systems

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Identify the origin of the potentially malicious root certificate
4. Perform Endpoint/AV scans on affected systems

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Credential Access - Password Spraying

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that workstations and servers are logging to a central location
4. Verify that authentication attempts to systems and applications are being logged
5. Set up network segmentation and firewalls to limit access to systems and services
6. Make use of multi-factor authentication
7. Establish and enforce a secure password policy

(I) Identification

1. Monitor for:
   a. Failed login attempts for default and common account names
   b. Failed login attempts for the same account across multiple systems
   c. Failed login attempts to multiple systems from the same source
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Review logs to determine if the attacker successfully logged in to any accounts
5. Lock any compromised accounts
6. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Reset the credentials of any compromised accounts
3. Inspect any potentially compromised assets

(R) Recovery

1. Restore to the RPO within the RTO
2. Resolve any related security incidents
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Collection - Email Collection - Cloud Email Compromise

(P) Preparation

1. Ensure client software is fully patched
2. Perform routine inspections of controls/weapons
3. Verify that logging and alerting are enabled and configured
4. Make use of risk based conditional access policies
5. Perform routine phishing education and testing
6. Familiarize yourself with the available security features of your service
7. Generate and review reports of logins on a regular basis
8. Ban the use of passwords that include your company's name or product names, if possible
9. Make use of a third party service to monitor for data breaches that include company email addresses

(I) Identification

1. Monitor for:
   a. Unusual login activity
   b. Changes to email forwarding rules
   c. Security features being disabled
   2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Review logs to determine if the attacker successfully accessed any other accounts
5. Lock any compromised accounts
6. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Reset the credentials of any compromised accounts
3. Inspect the workstations of compromised users

(R) Recovery

1. Restore to the RPO within the RTO
2. Resolve any related security incidents
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Persistence - BITS Jobs

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on systems
4. Ensure that servers and workstations are logging to a central location
5. Log network traffic

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS alerts
   d. The creation of new BITS jobs
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Review the suspicious BITS job
6. Lock any potentially compromised accounts
7. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on affected systems
4. Review logs to determine if any other systems are affected
5. Check for and remove other persistence mechanisms in place

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine how the BITS job was created
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Persistence - Pre-OS Boot

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations and laptops
4. Ensure that servers and workstations are logging to a central location
5. Set a BIOS or UEFI password on applicable assets
6. Use TPM technology and a trusted boot process
7. Secure local administrator accounts
8. Log any changes to boot records, BIOS, and EFI
9. Create backups of the bootloader partition

(I) Identification

1. Monitor for:
   a. Suspicious changes to boot files
   b. Unusual DNS activity
   c. Antivirus/Endpoint alerts
   d. IDS/IPS alerts
2. Compare boot records, configuration files, and firmware against known good images
3. Perform integrity checks of pre-OS boot mechanisms
4. Utilize disk checks, forensic utilities, and data from device drivers to identify anomalies
5. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Remove the affected system from the network
6. Verify the boot integrity of any other at-risk assets
7. Check network logs for suspicious egress traffic

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Create forensic backups of affected systems
4. Replace firmware and boot files from backups or trusted sources
5. Perform Endpoint/AV scans on affected systems

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident

4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Conduct employee security awareness training

Privilege Escalation - Group Policy Modification

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers and workstations are logging to a central location
4. Audit Group Policy Object (GPO) permissions periodically
5. Use WMI and Security group filtering to limit which systems and users GPOs will apply to

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. GPO creation, deletion, or modification e. Creation of scheduled tasks and services
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Lock compromised user accounts
5. Systems believed to have malware on them should be removed from the network
6. Review system logs to determine what changes the attacker made

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Create forensic backups of affected systems
4. Perform Endpoint/AV scans on affected systems
5. Audit Group Policy Objects and permissions

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Defense Evasion - Process Injection

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Secure local administrator accounts
5. Ensure that servers and workstations are logging to a central location
6. Configure endpoint security solutions to detect and block process injection behaviors
7. On Unix-based operating systems, restrict the use of ptrace to privileged users
8. Utilize Yama or other Linux security modules to configure advanced access control and process restrictions

(I) Identification

1. Monitor for:
    a. CreateRemoteThread
    b. SuspendThread
    c. SetThreadContext
    d. ResumeThread
    e. QueueUserAPC
    f. NtQueueApcThread
    g. VirtualAllocEx
    h. WriteProcessMemory
2. On Linux systems, monitor the ptrace system call
3. Detect named pipe creation and connection events
4. Collect DLL/PE file events
5. Analyze process behavior and compare to expected activity
6. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Conduct employee security awareness training

Privilege Escalation - Exploitation for Privilege Escalation

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Ensure that servers and workstations are logging to a central location
5. Make use of application sandboxing
6. Make use of exploit mitigation tools such as Windows Defender Exploit Guard
7. Ensure that good patch management practices are being followed

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alert
   c. IDS/IPS alerts
2. Activity preceding and following escalation attempts may produce detectable IOC
3. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Remove the affected system from the network
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Credential Access - OS Credential Dumping

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Limit credential overlap across accounts and systems
5. Ensure that servers and workstations are logging to a central location
6. Confirm that Domain Controller backups are properly secured
7. Avoid placing domain accounts in local administrator groups across systems
8. Add users to the "Protected Users" AD security group to limit the caching of plaintext credentials
9. Consider disabling WDigest authentication and disabling or restricting NTLM

(I) Identification

1. Monitor processes and command-line arguments for indicators of credential dumping
2. Identify unexpected processes interacting with lsass.exe
3. Detect Security Accounts Manager (SAM) access on the local file system
4. Monitor domain controller logs for replication requests and unscheduled activity
5. On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for lsass.exe and verify that it starts as a protected process
6. Investigate and clear ALL alerts associated with impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents

5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Conduct employee security awareness training

Credential Access - Unsecured Credentials

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Limit credential overlap across accounts and systems
5. Ensure that servers and workstations are logging to a central location
6. Implement password policies that:
   a. Require strong passphrases
   b. Prohibit password storage in the registry and within insecure files
   c. Recommend storing passwords on separate cryptographic hardware
7. Conduct employee security awareness training

(I) Identification

1. Watch processes and command-line arguments for indicators of credential searching
2. Monitor for:
   a. Unusual permission modification
   b. Abnormal file access
   c. Unexpected account creation
   d. Atypical reading of .bash_history
3. Investigate and clear ALL alerts associated with impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Remove the affected system from the network
5. Lock any accounts that exhibit suspicious behavior
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Review logs to determine which accounts were accessed
5. Inspect all affected accounts
6. Search file systems and logs to determine if insecure credentials were collected
7. Reset the passwords of any compromised accounts
8. Patch asset vulnerabilities
9. Remove all instances of credentials that were stored insecurely

(R) Recovery

1. Restore to the RPO within the RTO

2. Assess and Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk

Defense Evasion - Obfuscated Files or Information

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Employ a multifaceted approach to malware detection, that includes, but is not limited to:
   a. File-based detection
   b. Heuristic-based detection
   c. Network-based detection
   d. Behavior-based detection
   e. Reputation-based detection
5. Regularly update virus definitions and signatures
6. Ensure that servers and workstations are logging to a central location
7. Conduct employee security awareness training

(I) Identification

1. Flag and analyze commands that contain indicators of obfuscation or suspicious syntax
2. Use network intrusion detection systems (NIDS) and email gateway filtering to identify compressed/encrypted attachments and scripts
3. Utilize file scanning to look for known software packers and software packing techniques
4. Search system artifacts for steganography-related strings and signatures
5. Look for non-native binary formats, cross-platform compilers, and execution frameworks
6. Investigate and clear ALL alerts associated with impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage

3. Determine the root cause of the breach
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk

Impact - Disk Wipe

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Regularly update virus definitions and signatures
5. Take regular backups of critical systems and ensure the hardened storage is off-site or offline
6. Develop an IT disaster recovery plan
7. Utilize threat intelligence to make informed decisions about defensive priorities
8. Ensure that servers are logging to a central location
9. Conduct employee security awareness training
10. Be aware of any laws or contractual obligations that require notification of data loss

(I) Identification

1. Monitor for:
   a. Attempts to write to the MBR or partition table
   b. Unusual kernel driver activity
   c. Direct access to drives using the "\\.\" notation
   d. IDS/IPS alerts
   e. Antivirus alerts
   f. Unusual error messages in logs
   g. Unusual web traffic patterns
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations
8. Determine what data was stored on the device

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore affected systems to their last clean backup
3. Assess and Address collateral damage
4. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Persistence - Office Application Startup

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Conduct employee security awareness training
5. Disable add-ins and prevent Office VBA macros from executing
   a. If add-ins are necessary, follow best practices for securing them, such as requiring them to be signed
   b. NOTE: disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code
6. Ensure that servers and workstations are logging to a central location
7. Create the registry key for the Office Test [2] method and set the permissions to "Read Control"

(I) Identification

1. Monitor for:
   a. Abnormal chains of activity resulting from Office processes
   b. Events related to Registry key creation and modification
   c. Office processes performing anomalous DLL loads
   d. Changes to Office macro security settings or base templates
2. Check for the creation of the Office Test key
   a. TIP: Sysinternals Autoruns [3] can detect tasks set up using the Office Test Registry key
3. Audit Registry entries that are relevant to enabling add-ins
4. Validate Office trusted locations
5. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery

7. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Execution - User Execution

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Utilize threat intelligence to make informed decisions about defensive priorities
5. Conduct employee security awareness training
6. Consider restricting web-based content [1] that could be malicious such as:a. Javascriptb. Downloads from untrusted websitesc. Browser extensions
7. Use application control to whitelist approved applications [2]
8. Reference CIRT Playbook Battle Card: GSPBC-1002 - Credential Access - Spearphishing - Phishing [3]
9. Ensure that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
   a. Abnormal network activity
   b. Unauthorized downloads
   c. Emails with suspicious attachments
   d. IDS/IPS alerts
   e. Antivirus alerts
   f. Unusual executable files with the following file types: .exe, .doc, .pdf, .xls, .rtf, .scr, .lnk, .pif, and .cpl. [4]
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Reconnaissance - Active Scanning

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Verify that firewall, SIEM, IDS, and IPS appliances and software are up-to-date
6. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
7. Restrict access to RDP, SSH, and similar protocols
8. Remove default banners from remote connection protocols
9. Remove default headers from web application responses

(I) Identification

1. Monitor for:
   a. Excessive requests on public facing assets, especially if coming from a single source [1]
   b. Abnormal requests for public facing applications and protocols [1]
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts [2]
4. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Address any collateral damage by assessing exposed technologies
2. Resolve any related security incidents

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence

2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Persistence - Hijack Execution Flow

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Conduct employee security awareness training
5. Ensure all software is kept up to date
6. Restrict the loading of remote DLLs [1]
7. Restrict users to the least privileges required
8. Confirm that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
   a. Moving, renaming, replacing, or modifying of DLLs
   b. Applications loading DLLs not consistent with past behavior
   c. DLLs that have the same file name but abnormal paths
   d. Changes to environment variables e.
   Unusual process activity
   f. Suspicious modification or creation of .manifest and .local redirection files [2]
   2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on affected systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and Address collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Resource Development - Compromise Accounts

(P) Preparation

1. Patch asset vulnerabilities
2. Enforce strong password policies
   a. Don't allow the usage of old passwords
   b. Cycle passwords according to the organization's best practices
   c. Enforce alpha-numeric passwords, with symbols, and longer than 8 characters
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to RDP, SSH, and similar protocols
7. Conduct employee security awareness training
8. Restrict users to the least privileges required

(I) Identification

1. Monitor:
   a. Social media activity related to your organization [1]
   b. Suspicious emails and attachments coming into your organization [2]
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior [3]
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Credential Access - Input Capture

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Conduct employee security awareness training
5. Ensure all software is kept up to date
6. Restrict users to the least privileges required
7. Use application control to whitelist approved applications [1]
8. Confirm that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
   a. Abnormal program execution
   b. Malicious instances of Command and Scripting interpreters [2]
   c. Calls to the SetWindowsHookEx and SetWinEventHook functions [3]
   d. Rootkits
   e. Unauthorized drivers and kernel modules
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and address collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Execution - Native API

(P) Preparation

1. Patch asset vulnerabilities
2. Ensure antivirus/endpoint protection software is installed on workstations and laptops
3. Confirm that servers and workstations are logging to a central location
4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
5. Restrict access to critical assets as needed
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Identify and block potentially malicious software that may be executed through this technique by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate [1]

(I) Identification

1. Monitor:
   a. Social media activity related to your organization
   b. Suspicious emails and attachments coming into your organization
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts
5. Collect API call logs to analyze potentially malicious behavior. Correlation of activity by process lineage by process ID may be sufficient [2]
6. Monitor for unusual DLL loads or potentially malicious processes [2]

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents

4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Credential Access - Credentials from Password Stores

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Regularly update virus definitions and signatures
5. Conduct employee security awareness training
6. Ensure all software is kept up to date
7. Restrict users to the least privileges required
8. Utilize threat intelligence to make informed decisions about defensive priorities
9. Use application control to whitelist approved password storage applications [1]
10. Ensure that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
   a. Searches to process memory for common credential keywords, such as; password, pwd, login, store, secure, credentials, etc. [2]
   b. Automated tools scanning memory for passwords
   c. Storage of passwords in plaintext
   d. Abnormal activity around all authorized password storage applications
   e. Use of unauthorized password storage applications
   f. Access to web browser password storage database files [3]
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery

7. Patch asset vulnerabilities
8. Remove all instances of credentials that were stored insecurely
9. Reset the passwords of any compromised accounts

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Defense Evasion - Indirect Command Execution

(P) Preparation

1. Patch asset vulnerabilities
2. Ensure antivirus/endpoint protection software is installed on workstations and laptops
3. Confirm that servers and workstations are logging to a central location
4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
5. Restrict access to critical assets as needed
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Audit system controls, features, and programs that may indirectly use the command line or a terminal and restrict such features to only those necessary [1]

(I) Identification

1. Monitor for:
   a. Social media activity for unusual body posts or inconsistent server requests
   b. Suspicious emails and attachments coming into your organization
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts
5. Monitor and analyze logs from host-based detection mechanisms, such as Sysmon, for events such as process creations that include or are resulting from parameters associated with invoking programs/commands/files and/or spawning child processes/network connections Social media activity related to your organization [1]

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threatactor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents

4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Execution - Deploy Container

(P) Preparation

1. Use application control to whitelist approved applications [1]
2. Ensure that servers and workstations are logging to a central location
3. Deny direct remote access to internal systems [2]
4. Patch asset vulnerabilities
5. Perform routine inspections of controls/weapons
6. Ensure antivirus/endpoint protection software is installed on workstations and laptops
7. Regularly update virus definitions and signatures
8. Conduct employee security awareness training
9. Ensure all software is kept up to date
10. Restrict users to the least privileges required
11. Utilize threat intelligence to make informed decisions about defensive priorities

(I) Identification

1. Monitor for:
   a. Suspicious or unknown container images
   b. Unauthorized API calls
   c. Anomalous container activity
   d. Downloads of container images from unknown sources e. Unusual activity in container deployment logs [3]
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities
8. Reset the passwords of any compromised accounts

(R) Recovery

1. Restore to the RPO within the RTO

2. Assess and address collateral damage
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Credential Access - Steal Web Session Cookies

(P) Preparation

1. Patch asset vulnerabilities
2. Ensure antivirus/endpoint protection software is installed on workstations and laptops
3. Confirm that servers and workstations are logging to a central location
4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
5. Restrict access to critical assets as needed
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Configure browsers or tasks to delete persistent cookies regularly [1]
9. Consider setting up a physical second-factor key that uses the target login domain as part of the negotiation protocol [1]

(I) Identification

1. Monitor for:
   a. Attempts to access files and repositories on a local system that are used to store browser session cookies [1]
   b. Attempts by programs to inject into or dump browser process memory [1]
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Train users to identify aspects of phishing attempts where they're asked to enter credentials into a site that has the incorrect domain for the application they are logging into

Discovery - Process Discovery

(P) Preparation

1. Patch asset vulnerabilities
2. Ensure antivirus/endpoint protection software is installed on workstations and laptops
3. Confirm that servers and workstations are logging to a central location
4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
5. Restrict access to critical assets as needed
6. Conduct employee security awareness training
7. Restrict users to the least privileges required

(I) Identification

1. Monitor for:
   a. Malicious tasklist commands ran in Windows environment [1]
   b. Malicious ps commands ran in Mac and Linux environments [1]
   c. Actions that could be taken to gather system and network information [1]
   d. Attempts by programs to exfiltrate process memory [1]
2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior
3. Analyze web application metadata for suspicious user-agent strings and other artifacts
4. Investigate and clear ALL alerts
5. Investigate information provided by Windows Management Instrumentation and Windows API via PowerShell [1]

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities [1]

Lateral Movement - Replication Through Removable Media

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Limit the use of USB devices and removable media within a network
10. Block untrusted executables from running from removable media [1]

(I) Identification

1. Monitor for:
   a. Unusual file access on removable media [1]
   b. Processes that execute from removable media after it is mounted [1]
   c. Network connections to command and control servers [1]
   d. Processes involving unusual system and network information discovery [1]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that aren't supposed to be loaded by that process [1]

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Execution - Exploitation for Client Execution

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Consider running applications on virtual machines. [1]

(I) Identification

1. Monitor for:
   a. Abnormal browser or Office process behavior [2]
   b. Suspicious files written to disk [2]
   c. Log modification [2]
   d. Unusual network traffic [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Lateral Movement - Taint Shared Content

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Restrict access to shared drives to only employees requiring access [1]

(I) Identification

1. Monitor for:
   a. Suspicious processes writing or overwriting several files on a shared drive [2]
   b. Suspicious processes accessing shared drives without authorization [2]
   c. Network communications to C2 servers [2]
   d. Processes executing from removable media [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Temporarily remove access to the shared drive to limit further spread
3. Scan shared drives for malicious files or other files that do not belong in the shared drive [2]
4. Perform endpoint/AV scans on targeted systems
5. Reset any compromised passwords
6. Inspect ALL assets and user activity for IOC consistent with the attack profile
7. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
8. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore access to the shared drive to only employees requiring access
3. Address any collateral damage by assessing exposed technologies

4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals Implement policy changes to reduce future risk
3. Utilize newly obtained threat signatures
4. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Privilege Escalation - Create or Modify System Process

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them [1]

(I) Identification

1. Monitor for:
   a. Changes to system processes that do not correlate with known software, patch cycles, etc [2]
   b. Abnormal process call trees from known services [2]
   c. Abnormal changes to files associated with system-level processes [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Defense Evasion - Subvert Trust Controls

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Use application control and/or script blocking to block unapproved applications [1]
10. Ensure "Hide Microsoft Entries" and "Hide Windows Entries" are both deselected in Autoruns [2]
11. Utilize Windows Group Policy to manage root certificates [2]

(I) Identification

1. Monitor for:
   a. Abnormal attempts to modify extended file attributes with utilities such as “xattr” [2]
   b. Deviations in expected Autoruns activity [2]
   c. Unexpected certificates installed on a system [3]
   d. Deviations in registered SIPs and trust providers [2]
   e. Outliers in signing certificate metadata [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery

6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Defense Evasion - Domain Policy Modification

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Identify and correct GPO permissions abuse opportunities [1]
10. Consider implementing WMI and security filtering [1]

(I) Identification

1. Monitor for:
   a. Malicious scheduled tasks [2]
   b. Rogue Domain Controllers [2]
   c. Suspicious GPO changes [2]
   d. Commands/cmdlets and command-line arguments that may be leveraged to modify domain policy settings [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Credential Access - Brute Force

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Set lockout policies to lock accounts after a certain number of failed login attempts
10. Enable multi-factor authentication wherever possible
11. Use strong password policies on all accounts

(I) Identification

1. Monitor for high volumes of authentication failures through any of the following methods:
   a. Password guessing [1]
   b. Password Cracking [2]
   c. Password Spraying [3]
   d. Credential Stuffing [4]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Impact - Resource Hijacking

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required [1]
9. Review AUP and BYOD policies [1]

(I) Identification

1. Monitor for:
   a. Unusual process resource usage to determine anomalous activity associated with the malicious hijacking of computer resources such as CPU, memory, and graphics processing resources [1]
   b. Suspicious use of network resources associated with cryptocurrency mining software [1]
   c. Common cryptomining software process names and files on local systems that may indicate compromise and resource usage [1]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Initial Access - Hardware Additions

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Restrict network access to critical infrastructure and resources as needed [1]
9. Deny all access to removable media if not required for business operations

(I) Identification

1. Monitor for:
   a. Unauthorized use of external communication ports including the use of USB devices [2]
   b. Unauthorized additions of system hardware [3]
   c. Any assets that should not exist on the network
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately
8. Remove any unapproved removable media from the environment

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Exfiltration - Exfiltration Over Physical Medium

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Apply a Data Loss Prevention (DLP) strategy [1]
9. Disable Autorun if it is unnecessary [2]
10. Limit the use of USB devices and removable media within a network [3]

(I) Identification

1. Monitor for:
   a. Executed commands and arguments that may attempt to exfiltrate data via a physical medium [4]
   b. Newly assigned drive letters or mount points to a data storage device [4]
   c. Unauthorized file access on removable media [4]
   d. Newly executed processes when removable media is mounted [4]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately
8. Remove any unapproved removable media from the environment

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time

Objective)

2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Defense Evasion - Impair Defenses

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Ensure permissions are in place to restrict unauthorized users from interfering with security services [1]

(I) Identification

1. Monitor for:
   a. Unauthorized modifications to the Windows Registry [2]
   b. Unauthorized modifications to the firewall
   c. Unauthorized command or script execution [3] [4]
   d. Unauthorized process creation or termination [5]
   e. Unauthorized access or modification to security tools/weapons
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Initial Access - Exploit Public-Facing Application

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Implement Web Application Firewalls (WAFs) [1]
9. Segment externally facing servers and services from the rest of the network with a DMZ or by using separate hosting infrastructure [2]

(I) Identification

1. Monitor by:
   a. Using deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings, known payloads, and other indicators of compromise [3]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately
8. Remove any unapproved removable media from the environment

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents

4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Discovery - Password Policy Discovery

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Set and enforce secure password policies for all accounts [1]
9. Refer to NIST guidelines when creating password policies [2]
10. Ensure all accounts with elevated permissions have passwords that are unique, complex, and required to be changed periodically

(I) Identification

1. Monitor for:
   a. Access to detailed information about the organization's local password policy [3]
   b. Access to cloud-based password policies such as AWS [3]
   c. Multiple failed authentication attempts across one or various accounts
   d. Attempts by a user account to gain access to unusual or unauthorized systems or networks
   e. Sign-in failures from out-of-the-ordinary locations or repeated MFA failures
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities
7. Reset accounts that have been breached immediately

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Reconnaissance - Gather Victim Host Information

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Focus on minimizing the amount and sensitivity of data available to external parties [1]

(I) Identification

1. Monitor for:
   a. Logged network traffic in response to a scan showing both protocol header and body values that may buy and/or steal SSL/TLS certificates that can be used during targeting [2]
   b. Contextual data about an Internet-facing resource gathered from a scan, such as running services or ports that may buy, lease, rent, or compromise infrastructure that could be used during targeting [2]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery

6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Defense Evasion - Valid Accounts

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation and log between segments
5. Incorporate threat intelligence
6. Perform routine inspections of asset backups
7. Conduct user security awareness training (with a focus on suspicious MFA activity awareness) [1]
8. Conduct response training (this PBC)
9. Ensure applications are storing credentials in a secure manner and enforce credential updates at regular intervals [1]
10. Immediately change default account credentials [1]
11. Adhere to the principle of least privilege [1]
12. Perform regular sweeps for inactive user accounts and verify they are purged from the environment [1]

(I) Identification

1. Monitor for:
    a. Abnormalities or potential abuse of existing user credentials [2]
    b. Suspicious account behavior across systems that share accounts [3]
    c. Newly created accounts gaining access to unauthorized systems or software [3]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Persistence - Modify Authentication Process

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Enable multi-factor authentication on all authentication interfaces [1]
12. Disallow passwords to be stored using reversible encryption [1]

(I) Identification

1. Monitor for:
   a. changes made to AD security settings related to MFA logon requirements [1]
   b. newly constructed logon behavior across systems that shared accounts, either user, admin, or service accounts [1]
   c. new, unfamiliar DLL files written to a domain controller and/or local computer [1]
   d. suspicious additions to the /Library/Security/SecurityAgentPlugins directory [1]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assetsDisable privileges for accounts suspected of compromise [1]

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Discovery - Browser Bookmark Discovery

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Log traffic between network segments
5. Incorporate threat intelligence
6. Perform routine inspections of asset backups
7. Conduct phishing simulations
8. Conduct user security awareness training
9. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
   a. Executed commands or actions taken to gather browser bookmark information via remote access tools, system management tools, or Powershell [1]
   b. Unexpected access or viewing of browser bookmarks [1]
   c. Collection or exfiltration of browser bookmark data [1]
   d. New processes unexpectedly gathering personal user data [1]
   2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets
8. Disable privileges for accounts suspected of compromise [1]

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Command and Control - Application Layer Protocol

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Implement signature-based network intrusion detection and prevention systems [3]

(I) Identification

1. Monitor for:
   a. Newly constructed network connections that are sent or received by untrusted hosts [2]
   b. Processes utilizing the network that do not normally have network communication or have never been seen before [2]
   c. Unexpected protocol standards and traffic flows [2]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)

2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Pay attention to unusual behavior exhibited by trusted parties
8. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Execution - Scheduled Task or Job

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Regularly update virus definitions and signatures
5. Conduct employee security awareness training
6. Ensure all software is kept up to date
7. Audit for permission weaknesses that could be used to escalate privileges [4]
8. Leverage GPO to force tasks to run under an authenticated account [2]
9. Restrict scheduled tasks to a defined group of administrators [3]

(I) Identification

1. Monitor for:
   a. Existing commands that may abuse task scheduling functionality to execute malicious code [1]
   b. Newly constructed containers or files that may abuse task scheduling to execute malicious code [1]
   c. Newly created scheduled jobs for initial indicators of malicious activity [1]
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on targeted systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities
8. Reset the passwords of any compromised accounts

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Assess and address collateral damage

3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

Persistence - Event Triggered Execution

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
   a. Suspicious configurations on the local system such as newly constructed files or WMI objects, modified registry keys, or unrecognized DLL activity [1]
   b. Creation or modification of cloud-based function and workflow monitoring services [3]
   2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity
4. Utilize Sysinterals Autoruns to view programs configured to run in response to startup or application execution [2]

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)

2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Pay attention to unusual behavior exhibited by trusted parties
8. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Initial Access - Replication Through Removable Media

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Enable Attack Surface Reduction rules to block unsigned/untrusted executable files. [4]
12. Disable Autorun if it is unnecessary. [5]

(I) Identification

1. Monitor for:
   a. newly constructed drive letters or mount points to removable media [1]
   b. unexpected or newly constructed files on removable media [2]
   c. executed processes originating from removable media [3]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)

2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

Persistence - Scheduled Task or Job

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled [4]
9. Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority [5]
10. Conduct phishing simulations
11. Conduct user security awareness training
12. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
   a. executed commands and arguments and newly constructed containers that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code [1]
   b. newly constructed files and changes made to files that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code [2]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity
4. threat groups, such as Earth Lusca, have been known to establish persistence using the following command: schtasks /Create /SC ONLOgon /TN Windows UpdateCheck /TR '[filepath]' /ru [6]
5. Utilize Sysinterals Autoruns to view programs configured to run in response to startup or application execution [2]

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack

7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Pay attention to unusual behavior exhibited by trusted parties
8. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities
9. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges [3]

Credential Access - Network Sniffing

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS. [1]
12. Use multi-factor authentication wherever possible. [2]
13. In cloud environments, ensure that users are not granted permissions to create or modify traffic mirrors unless this is explicitly required. [3]

(I) Identification

1. Monitor for:
   a. executed commands and arguments for actions that aid in sniffing network traffic to capture information about an environment, including authentication material passed over the network [4]
   b. newly executed processes that can aid in sniffing network traffic to capture information about an environment, including authentication material passed over the network [5]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity
4. Utilize Sysinterals Autoruns to view programs configured to run in response to startup or application execution [2]

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems

3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
3. Restore affected systems to their last clean backup

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Pay attention to unusual behavior exhibited by trusted parties
8. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities